



HEALTH AFFAIRS



HIPAA Security Topics - 2

Web Resources, Implementation Guide and Biomedical Devices

HIPAA Training: 2005 Summer Sessions

TMA Privacy Office

*This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.*

Agenda

- TMA Privacy Office HIPAA Security Web Site
- Risk Information Management Resource (RIMR)
- HIPAA Security Implementation Guide
- Biomedical Devices

Training Objectives

- Upon completion of this course you will be able to:
 - Identify available resources to aid in Security Awareness
 - Identify available training briefings
 - Identify available resources to aid in implementation of HIPAA Security
 - Describe the relationship between HIPAA Security and biomedical devices

TMA Privacy Office HIPAA Security Web Site

TMA HIPAA Security Web Site

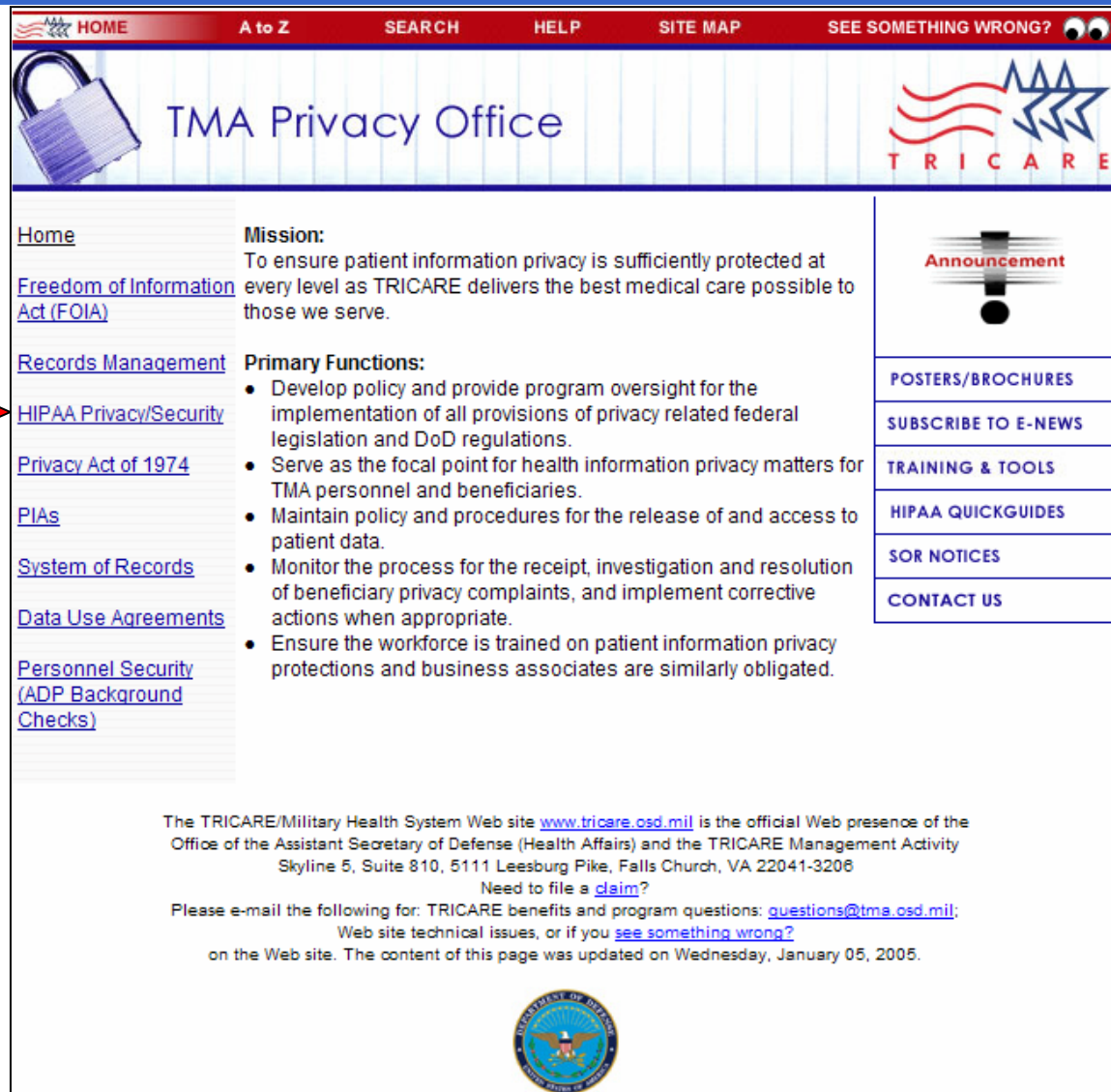
Objectives

- Upon completion of this lesson, you will be able to:
 - Locate information pertaining to security topics and HIPAA security management
 - Locate information pertaining to HIPAA support tools and training
 - Locate information pertaining to HIPAA news, conferences and e-news

TMA HIPAA Security Web Site

<http://www.tricare.osd.mil/tmaprivacy>

(1 of 3)



HOME A to Z SEARCH HELP SITE MAP SEE SOMETHING WRONG?

TMA Privacy Office

Mission:
To ensure patient information privacy is sufficiently protected at every level as TRICARE delivers the best medical care possible to those we serve.

Primary Functions:


- Develop policy and provide program oversight for the implementation of all provisions of privacy related federal legislation and DoD regulations.
- Serve as the focal point for health information privacy matters for TMA personnel and beneficiaries.
- Maintain policy and procedures for the release of and access to patient data.
- Monitor the process for the receipt, investigation and resolution of beneficiary privacy complaints, and implement corrective actions when appropriate.
- Ensure the workforce is trained on patient information privacy protections and business associates are similarly obligated.

Announcement

POSTERS/BROCHURES
SUBSCRIBE TO E-NEWS
TRAINING & TOOLS
HIPAA QUICKGUIDES
SOR NOTICES
CONTACT US

The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity
Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206
Need to file a [claim](#)?


Please e-mail the following for: TRICARE benefits and program questions: questions@tma.osd.mil;
Web site technical issues, or if you [see something wrong?](#)
on the Web site. The content of this page was updated on Wednesday, January 05, 2005.





TMA HIPAA Security Web Site

<http://www.tricare.osd.mil/tmaprivacy>

(2 of 3)

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [SITE MAP](#) [SEE SOMETHING WRONG?](#) 


 **TMA Privacy Office
HIPAA Compliance** 


[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[PIAs](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

Purpose:

To implement and monitor compliance with the HIPAA Privacy Rule, DoD 6025.18-R, "DoD Health Information Privacy Regulation" 24 January 2003 and coordinate the resolution of privacy related security issues.

The HIPAA Compliance Division develops, implements and monitors associated program policy. The division screens information requests and executes those that can be fulfilled under the HIPAA Privacy and Security Rules. The division will forward requests to appropriate subject matter offices, as needed. The division ensures all time-sensitive inquiries are addressed appropriately and conducts compliance monitoring and audits.


HIPAA Privacy


HIPAA Security


The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206

Need to file a [claim](#)?

Please e-mail the following for: TRICARE benefits and program questions: questions@tma.osd.mil; Web site technical issues, or if you [see something wrong?](#) on the Web site. The content of this page was updated on Wednesday, January 05, 2005.



TMA HIPAA Security Web Site

<http://www.tricare.osd.mil/tmaprivacy>

(3 of 3)

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)



Security Awareness Campaign

Check out the new [Password Management](#) poster for this month which can be found on the [Posters/Brochures](#) page.

Additional Resources

- [Security Awareness and Training](#)
- [Access Controls](#)
- [Person and Entity Authentication](#)
- [Information Access Management](#)

Important Message- HIPAA BASICS!

New upgrades are being made to HIPAA BASICS, including the structure of the database, the process for compliance assessment reporting and new reports. Once implemented, enhanced reporting capabilities will be available that allow users to generate aggregate reports. A large portion of these upgrades involve the creation of new subscriptions and the movement of current gaps into a new hierarchy. The target dates for the migration to this new hierarchy is May 21, 2005 through May 24, 2005. **The HIPAA BASICS application will not be available during this time period.** In order to ensure that no gaps are lost during this transition we ask that no one create **new gaps, add new lead users, or reassign lead users after May 17, 2005**, until the upgrade is complete and the application is back on line. You may continue to work on gaps that already exist during the period between May 17, 2005 and May 21, 2005 when the application goes off line.

[The State of HIPAA Privacy and Security Compliance, April 2005 \(Survey\)](#)

AHIMA has once again surveyed healthcare privacy officers and others whose jobs relate to HIPAA and relates to compliance with both the privacy and security rules. The results of the survey will reinforce the importance of protecting personal health information and help the industry to understand the areas of privacy and security implementation that are most difficult and may need more study.



- [SECURITY HOMEPAGE](#)
- [PRIVACY HOMEPAGE](#)
- [TMA GUIDANCE](#)
- [INFO LIBRARY](#)
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)



MHS Information Assurance (IA) Policy/Guidance Manual
March 5, 2004




Email Disclaimer Statement


TMA HIPAA Security Web Site

TMA Guidance (1 of 2)


[HOME](#)
[A to Z](#)
[SEARCH](#)
[HELP](#)
[WHAT'S NEW](#)
[SITE MAP](#)



TMA Privacy Office
HIPAA Compliance: Security




[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)




Security Awareness Campaign
Check out the new [Password Management](#) poster for this month which can be found on the [Posters/Brochures](#) page.

Additional Resources
[Security Awareness and Training](#)
[Access Controls](#)
[Person and Entity Information Access](#)
[Information Papers](#)
[Information Briefings](#)
[Policy Memos](#)
[Appointment Letters](#)
[BA Agreements](#)


Important Message- HIPAA BASICS
New upgrades are being made to the structure of the database, the process of reporting and new reports. Once implemented, enhanced reporting capabilities will be available that allow users to generate aggregate reports. A large portion of these upgrades involve the creation of new subscriptions and the movement of current gaps into a new hierarchy. The target dates for the migration to this new hierarchy is May 21, 2005 through May 24, 2005. **The HIPAA BASICS application will not be available during this time period.** In order to ensure that no gaps are lost during this transition we ask that no one create **new gaps, add new lead users, or reassign lead users after May 17, 2005**, until the upgrade is complete and the application is back on line. You may continue to work on gaps that already exist during the period between May 17, 2005 and May 21, 2005 when the application goes off line.


[The State of HIPAA Privacy and Security Compliance, April 2005 \(Survey\)](#) 

AHIMA has once again surveyed healthcare privacy officers and others whose jobs relate to HIPAA and relates to compliance with both the privacy and security rules. The results of the survey will reinforce the importance of protecting personal health information and help the industry to understand the areas of privacy and security implementation that are most difficult and may need more study.



[SECURITY HOMEPAGE](#)
[PRIVACY HOMEPAGE](#)
[TMA GUIDANCE](#)
[INFO LIBRARY](#)
[NEWS & CONFERENCES](#)
[TRAINING AND TOOLS](#)
[SECURITY IPT](#)
[POSTERS/BROCHURES](#)
[FAQs](#)
[LINKS](#)
[CONTACT US](#)

 **MHS Information Assurance (IA) Policy/Guidance Manual March 5, 2004**

 **Email Disclaimer Statement**


TMA HIPAA Security Web Site


TMA Guidance (2 of 2)

- Information Papers
 - HIPAA Security Overview and 25 other related information papers
- Information Briefings
 - Conference and informational briefings
- Policy Memos
 - Policy memos relating to HIPAA Security implementation
- Appointment Letters
 - MTF/DTF, TRICARE Regional Office and Service Headquarters
- BA Agreements
 - Joint HIPAA Privacy and Security contract clause


TMA HIPAA Security Web Site

Information Papers (1 of 2)


 HOME
 [A to Z](#)
[SEARCH](#)
[HELP](#)
[WHAT'S NEW](#)
[SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)



Security Awareness Campaign

Check out the new [Password Management](#) poster for this month which can be found on the [Posters/Brochures](#) page.

Additional Resources


- [Security Awareness and Training](#)
- [Access Controls](#)
- [Person and Entity Information Access](#)
- Information Papers**
- [Information Briefings](#)
- [Policy Memos](#)
- [Appointment Letters](#)
- [BA Agreements](#)

Important Message- HIPAA BASICS


New upgrades are being made to the structure of the database, the process reporting and new reports. Once implemented, enhanced reporting capabilities will be available that allow users to generate aggregate reports. A large portion of these upgrades involve the creation of new subscriptions and the movement of current gaps into a new hierarchy. The target dates for the migration to this new hierarchy is May 21, 2005 through May 24, 2005. **The HIPAA BASICS application will not be available during this time period.** In order to ensure that no gaps are lost during this transition we ask that no one create **new gaps, add new lead users, or reassign lead users after May 17, 2005**, until the upgrade is complete and the application is back on line. You may continue to work on gaps that already exist during the period between May 17, 2005 and May 21, 2005 when the application goes off line.

The State of HIPAA Privacy and Security Compliance, April 2005 (Survey)


AHIMA has once again surveyed healthcare privacy officers and others whose jobs relate to HIPAA and relates to compliance with both the privacy and security rules. The results of the survey will reinforce the importance of protecting personal health information and help the industry to understand the areas of privacy and security implementation that are most difficult and may need more study.



- [SECURITY HOMEPAGE](#)
- [PRIVACY HOMEPAGE](#)
- [TMA GUIDANCE](#)
- [INFO LIBRARY](#)
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)









MHS Information Assurance (IA) Policy/Guidance Manual
March 5, 2004




Email Disclaimer Statement


TMA HIPAA Security Web Site

Information Papers (2 of 2)


 HOME
  A to Z
  SEARCH
  HELP
  WHAT'S NEW
  SITE MAP




TMA Privacy Office
HIPAA Compliance: Security





[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Compliance](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

Information Papers
[Encryption of E-mail \(pdf\)](#) 
[Overview of Security Rule \(pdf\)](#)
[Who, What, When and Where of the Security Rule \(pdf\)](#)
[Standards and Implementation Specifications \(pdf\)](#)
[Policies and Procedures \(pdf\)](#)
[Documentation \(pdf\)](#)
[Administrative Safeguards \(pdf\)](#)
[Security Management Process \(pdf\)](#)
[Assigned Security Responsibility \(pdf\)](#)
[Workforce Security \(pdf\)](#)
[Information Access Management \(pdf\)](#)
[Security Awareness and Training \(pdf\)](#)
[Security Incident Procedures \(pdf\)](#)
[Contingency Plan \(pdf\)](#)
[Security Evaluation \(pdf\)](#)
[Business Associate Contracts and Other Arrangements \(pdf\)](#)
[Physical Safeguards \(pdf\)](#)
[Facility Access Control \(pdf\)](#)
[Workstation Use \(pdf\)](#)
[Workstation Security \(pdf\)](#)
[Device and Media Controls \(pdf\)](#)
[Technical Safeguards \(pdf\)](#)
[Access Controls \(pdf\)](#)
[Audit Controls \(pdf\)](#)
[Integrity Standards \(pdf\)](#)
[Person or Entity Authentication \(pdf\)](#)
[Transmission Security \(pdf\)](#)



[SECURITY HOMEPAGE](#)
[PRIVACY HOMEPAGE](#)
[TMA GUIDANCE](#)
[INFO LIBRARY](#)
[NEWS & CONFERENCES](#)
[TRAINING AND TOOLS](#)
[SECURITY IPT](#)
[POSTERS/BROCHURES](#)
[FAQs](#)
[LINKS](#)
[CONTACT US](#)


MHS
Information Assurance (IA)
Policy/
Guidance
Manual
March 5, 2004


Email
Disclaimer
Statement

[Top](#)

The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity
 Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206
 Please e-mail the following for: TRICARE benefits and program questions: questions@tma.osd.mil
 Web site technical issues, or if you : [see something wrong](#)
 The content of this page was updated on Wednesday, May 25, 2005.

TMA HIPAA Security Web Site

Information Briefings (1 of 2)

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Compliance](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

Information Papers

[Encryption of E-mail](#) (pdf) 
[Overview of Security Rule](#) (pdf)
[Who, What, When and Where of the Security Rule](#) (pdf)
[Standards and Implementation Specifications](#) (pdf)
[Policies and Procedures](#) (pdf)
[Documentation](#) (pdf)
[Administrative Safeguards](#) (pdf)
[Security Management Process](#) (pdf)
[Assigned Security Responsibility](#) (pdf)
[Workforce Security](#) (pdf)
[Information Access Management](#) (pdf)
[Security Awareness and Training](#) (pdf)
[Security Incident Procedures](#) (pdf)
[Contingency Plan](#) (pdf)
[Security Evaluation](#) (pdf)
[Business Associate Contracts and Other Arrangements](#) (pdf)
[Physical Safeguards](#) (pdf)
[Facility Access Control](#) (pdf)
[Workstation Use](#) (pdf)
[Workstation Security](#) (pdf)
[Device and Media Controls](#) (pdf)
[Technical Safeguards](#) (pdf)
[Access Controls](#) (pdf)
[Audit Controls](#) (pdf)
[Integrity Standards](#) (pdf)
[Person or Entity Authentication](#) (pdf)
[Transmission Security](#) (pdf)

[Top](#)



- [SECURITY HOMEPAGE](#)
- [POLICY HOMEPAGE](#)
- [TMA GUIDANCE](#)
- [INFO LIBRARY](#)
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)



MHS
Information Assurance (IA)
Policy/
Guidance
Manual
March 5, 2004




Email
Disclaimer
Statement

The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity
Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206
Please e-mail the following for: TRICARE benefits and program questions: questions@tma.osd.mil
Web site technical issues, or if you : [see something wrong](#)
The content of this page was updated on Wednesday, May 25, 2005.


TMA HIPAA Security Web Site

Information Briefings (2 of 2)

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)




TMA Privacy Office HIPAA Compliance: Security




[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Compliance](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

Information Briefings


[HIPAA Security: Meeting Compliance](#) (pdf) - 2005 TRICARE Conference
[HIPAA Security Overview](#) (ppt) - May 2004
[Compliance through Risk Management](#) (ppt) - May 2004
[DITSCAP/Fisma/HIPAA Security Crosswalk](#)
[Health Insurance Portability and Accountability Act \(HIPAA\) Security Requirements March, 2003](#) (ppt)
[HIPAA Privacy and Security Crosswalk](#) (ppt)
[HIPAA Security, TRICARE West Coast Conference, 2003](#) (ppt)
[HIPAA Security Brief- TRICARE Conference, 2003](#) (ppt)



- [SECURITY HOMEPAGE](#)
- [PRIVACY HOMEPAGE](#)
- [TMA GUIDANCE](#)
- [INFO LIBRARY](#)
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)



MHS
Information Assurance (IA)
Policy/
Guidance
Manual
March 5, 2004



Email
Disclaimer
Statement

The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity
Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3208
Please e-mail the following for: TRICARE benefits and program questions: questions@tma.osd.mil
Web site technical issues, or if you : [see something wrong](#)
The content of this page was updated on Wednesday, April 27, 2005.

TMA HIPAA Security Web Site

Policy Memos (1 of 2)

HOME
 [A to Z](#)
[SEARCH](#)
[HELP](#)
[WHAT'S NEW](#)
[SITE MAP](#)

[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Compliance](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

Information Papers

[Encryption of E-mail \(pdf\)](#)
[Overview of Security Rule \(pdf\)](#)
[Who, What, When and Where of the Security Rule \(pdf\)](#)
[Standards and Implementation Specifications \(pdf\)](#)
[Policies and Procedures \(pdf\)](#)
[Documentation \(pdf\)](#)
[Administrative Safeguards \(pdf\)](#)
[Security Management Process \(pdf\)](#)
[Assigned Security Responsibility \(pdf\)](#)
[Workforce Security \(pdf\)](#)
[Information Access Management \(pdf\)](#)
[Security Awareness and Training \(pdf\)](#)
[Security Incident Procedures \(pdf\)](#)
[Contingency Plan \(pdf\)](#)
[Security Evaluation \(pdf\)](#)
[Business Associate Contracts and Other Arrangements \(pdf\)](#)
[Physical Safeguards \(pdf\)](#)
[Facility Access Control \(pdf\)](#)
[Workstation Use \(pdf\)](#)
[Workstation Security \(pdf\)](#)
[Device and Media Controls \(pdf\)](#)
[Technical Safeguards \(pdf\)](#)
[Access Controls \(pdf\)](#)
[Audit Controls \(pdf\)](#)
[Integrity Standards \(pdf\)](#)
[Person or Entity Authentication \(pdf\)](#)
[Transmission Security \(pdf\)](#)

[Top](#)

[SECURITY MANAGEMENT](#)
[PRIVACY HOMEPAGE](#)
[TRANSPARENCY](#)
[TOOL LIBRARY](#)
[NEWS & CONFERENCES](#)
[TRAINING AND TOOLS](#)
[SECURITY IPT](#)
[POSTERS/BROCHURES](#)
[FAQs](#)
[LINKS](#)
[CONTACT US](#)

MHS Information Assurance (IA) Policy/Guidance Manual
March 5, 2004

Email Disclaimer Statement

The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206


Please e-mail the following for: TRICARE benefits and program questions: questions@tma.osd.mil
 Web site technical issues, or if you : [see something wrong](#)

The content of this page was updated on Wednesday, May 25, 2005.


TMA HIPAA Security Web Site

Policy Memos (2 of 2)

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)




TMA Privacy Office
HIPAA Compliance: Security




[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Compliance](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)


Policy Memos
[Memo: Use of HIPAA Basics](#)



- [SECURITY HOMEPAGE](#)
- [PRIVACY HOMEPAGE](#)
- [TMA GUIDANCE](#)
- [INFO LIBRARY](#)
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)



MHS Information Assurance (IA) Policy/Guidance Manual
March 5, 2004



Email Disclaimer Statement

The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206


Please e-mail the following for: TRICARE benefits and program questions: questions@tma.osd.mil
Web site technical issues, or if you : [see something wrong](#)

The content of this page was updated on Wednesday, April 27, 2005.


TMA HIPAA Security Web Site

Appointment Letters (1 of 2)

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)




TMA Privacy Office
HIPAA Compliance: Security





[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Compliance](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

Policy Memos

[Memo: Use of HIPAA Basics](#)



| | |
|-----------------------|---|
| Information Papers | SECURITY HOMER |
| Information Briefings | PRIVACY HOMER |
| Policy Memos | TMA GUIDANCE |
| Appointment Letters | INFORMATIONARY |
| BA Agreements | NEWS & CONFERENCES |
| | TRAINING AND TOOLS |
| | SECURITY IPT |
| | POSTERS/BROCHURES |
| | FAQs |
| | LINKS |
| | CONTACT US |
| |  MHS Information Assurance (IA) Policy/Guidance Manual March 5, 2004 |
| |  Email Disclaimer Statement |

The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206

Please e-mail the following for: TRICARE benefits and program questions: questions@tma.osd.mil

Web site technical issues, or if you : [see something wrong](#)

The content of this page was updated on Wednesday, April 27, 2005.

TMA HIPAA Security Web Site

Appointment Letters (2 of 2)

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)

[Freedom of Information Act \(FOIA\)](#)

[Records Management](#)

[HIPAA Compliance](#)

[Privacy Act of 1974](#)

[System of Records](#)

[Data Use Agreements](#)


[Personnel Security \(ADP Background Checks\)](#)

Appointment Letters


As the Privacy Rule required the appointment of a HIPAA Privacy Officer at the TRICARE Management Activity (TMA), Lead Agent and military treatment facility/dental treatment facility (MTF/DTF) levels, the Security Rule also requires an assignment of responsibilities. The MHS HIPAA Security Working Integrated Process Team (WIPT) and the HIPAA Security Program Officer have finalized Appointment (or Designation) Letters for the HIPAA Security Officers.

Please see the Appointment Letters below:


- [MTF/DTF](#)
- [TRICARE Regional Office](#)
- [Service Headquarters](#)



- [SECURITY HOMEPAGE](#)
- [PRIVACY HOMEPAGE](#)
- [TMA GUIDANCE](#)
- [INFO LIBRARY](#)
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)



MHS
Information
Assurance (IA)
Policy/
Guidance
Manual
March 5, 2004




Email
Disclaimer
Statement

The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity
Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206
Please e-mail the following for: TRICARE benefits and program questions: questions@tma.osd.mil
Web site technical issues, or if you : [see something wrong](#)
The content of this page was updated on Wednesday, April 27, 2005.


TMA HIPAA Security Web Site

BA Agreements (1 of 2)

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security




[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Compliance](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)



Appointment Letters

As the Privacy Rule required the appointment of a HIPAA Privacy Officer at the TRICARE Management Activity (TMA), Lead Agent and military treatment facility/dental treatment facility (MTF/DTF) levels, the Security Rule also requires an assignment of responsibilities. The MHS HIPAA Security Working Integrated Process Team (WIPT) and the HIPAA Security Program Officer have finalized Appointment (or Designation) Letters for the HIPAA Privacy Officer.

Please see the Appointment Letters

- [MTF/DTF](#)
- [TRICARE Regional Office](#)
- [Service Headquarters](#)



- [SECURITY HOMEPAGE](#)
- [PRIVACY HOMEPAGE](#)
- [TMA GUIDANCE](#)
- [INFO LISTS](#)
- [MEETINGS AND CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)
-  **MHS Information Assurance (IA) Policy/Guidance Manual March 5, 2004**
-  **Email Disclaimer Statement**

[Information Papers](#)
[Information Briefings](#)
[Policy Memos](#)
[Appointment Letters](#)
[BA Agreements](#)

The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206

Please e-mail the following for: TRICARE benefits and program questions: questions@tma.osd.mil


Web site technical issues, or if you : [see something wrong](#)

The content of this page was updated on Wednesday, April 27, 2005.


TMA HIPAA Security Web Site

BA Agreements (2 of 2)

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Compliance](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)


BA AGREEMENTS


A business associate (BA) is a person or entity who provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of protected health information (PHI). A business associate is not a member of the healthcare provider or covered entity's workforce.


Since the standards of the HIPAA Security Rule are intended to reinforce the privacy protections established by the Privacy Rule, the business associate agreements standard incorporated by the Security Rule is similar in scope and structure to that found in the Privacy Rule. As stated by the final Security Rule, a contract between a covered entity and a business associate must:

- Implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity
- Ensure that any agent, including a subcontractor, agrees to implement reasonable and appropriate safeguards
- Report to the covered entity any security incident of which it becomes aware
- Make its policies and procedures, and documentation available for purposes of determining the covered entity's compliance
- Authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract


The following clause may be included in contracts which involve the handling of protected health information by MHS business associates.

[Business Associate Contract Clause](#) (pdf) 


[Business Associate Contract Clause](#) (doc) 



[SECURITY HOMEPAGE](#)
[PRIVACY HOMEPAGE](#)
[TMA GUIDANCE](#)
[INFO LIBRARY](#)
[NEWS & CONFERENCES](#)
[TRAINING AND TOOLS](#)
[SECURITY IPT](#)
[POSTERS/BROCHURES](#)
[FAQs](#)
[LINKS](#)
[CONTACT US](#)




MHS
Information
Assurance (IA)
Policy/
Guidance
Manual
March 5, 2004




Email
Disclaimer
Statement


TMA HIPAA Security Web Site

Information Library (1 of 2)



[HOME](#)
[A to Z](#)
[SEARCH](#)
[HELP](#)
[WHAT'S NEW](#)
[SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)



Security Awareness Campaign


Check out the new [Password Management](#) poster for this month which can be found on the [Posters/Brochures](#) page.

Additional Resources


- [Security Awareness and Training](#)
- [Access Controls](#)
- [Person and Entity Information Access](#)
- Security Definitions**
- Final Rule**
- Info Articles**
- Policy/Guidance**

Important Message- HIPAA BASICS


New upgrades are being made to the structure of the database, the process of reporting and new reports. Once implemented, enhanced reporting capabilities will be available that allow users to generate aggregate reports. A large portion of these upgrades involve the creation of new subscriptions and the movement of current gaps into a new hierarchy. The target dates for the migration to this new hierarchy is May 21, 2005 through May 24, 2005. **The HIPAA BASICS application will not be available during this time period.** In order to ensure that no gaps are lost during this transition we ask that no one create **new gaps, add new lead users, or reassign lead users after May 17, 2005**, until the upgrade is complete and the application is back on line. You may continue to work on gaps that already exist during the period between May 17, 2005 and May 21, 2005 when the application goes off line.

[The State of HIPAA Privacy and Security Compliance, April 2005 \(Survey\)](#) 


AHIMA has once again surveyed healthcare privacy officers and others whose jobs relate to HIPAA and relates to compliance with both the privacy and security rules. The results of the survey will reinforce the importance of protecting personal health information and help the industry to understand the areas of privacy and security implementation that are most difficult and may need more study.



- [SECURITY HOMEPAGE](#)
- [PRIVACY HOMEPAGE](#)
- [TMA GUIDANCE](#)
- INFO LIBRARY**
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)



MHS
Information
Assurance (IA)
Policy/
Guidance
Manual
March 5, 2004



Email
Disclaimer
Statement

TMA HIPAA Security Web Site

Information Library (2 of 2)

- Security Definitions
 - HIPAA definitions list
- Final Rule
 - 45 CFR Parts 160, 162, and 164
- Info Articles
 - Information articles covering various security topics
- Policy and Guidance
 - DoD, Service-specific, and other Federal policy documentation

TMA HIPAA Security Web Site

Security Definitions (1 of 2)


[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)



Security Awareness Campaign


Check out the new [Password Management](#) poster for this month which can be found on the [Posters/Brochures](#) page.

Additional Resources


- [Security Awareness and Training](#)
- [Access Controls](#)
- [Person and Entity Information Access](#)
- Security Definitions**
- [Final Rule](#)
- [Info Articles](#)
- [Policy/Guidance](#)

Important Message- HIPAA BASICS


New upgrades are being made to the structure of the database, the process of reporting and new reports. Once implemented, enhanced reporting capabilities will be available that allow users to generate aggregate reports. A large portion of these upgrades involve the creation of new subscriptions and the movement of current gaps into a new hierarchy. The target dates for the migration to this new hierarchy is May 21, 2005 through May 24, 2005. **The HIPAA BASICS application will not be available during this time period.** In order to ensure that no gaps are lost during this transition we ask that no one create **new gaps, add new lead users, or reassign lead users after May 17, 2005**, until the upgrade is complete and the application is back on line. You may continue to work on gaps that already exist during the period between May 17, 2005 and May 21, 2005 when the application goes off line.

[The State of HIPAA Privacy and Security Compliance, April 2005 \(Survey\)](#) 

AHIMA has once again surveyed healthcare privacy officers and others whose jobs relate to HIPAA and relates to compliance with both the privacy and security rules. The results of the survey will reinforce the importance of protecting personal health information and help the industry to understand the areas of privacy and security implementation that are most difficult and may need more study.



- [SECURITY HOME PAGE](#)
- [PRIVACY HOME PAGE](#)
- [POLICY GUIDANCE](#)
- [INFO LIBRARY](#)
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)



MHS
Information
Assurance (IA)
Policy/
Guidance
Manual
March 5, 2004



Email
Disclaimer
Statement

TMA HIPAA Security Web Site

Security Definitions (2 of 2)

 HOME

A to Z

SEARCH

HELP

WHAT'S NEW

SITE MAP



TMA Privacy Office
HIPAA Compliance: Security



HIPAA PRIVACY DEFINITIONS

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

[A](#)

Access
The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Access Authorization
Under HIPAA, implementing policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

Access control
Under HIPAA, implementing policies and procedures for electronic information systems that contain EPHI electronic protected health information to only allow access to persons or software programs that have appropriate access rights.

Access Control and Validation Procedures
Under HIPAA, implementing procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing revision.

Access Establishment and Modification
Under HIPAA, the security policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program or process.

Access Level
A level rank or category label associated with an individual who may be accessing information (for example, a clearance level) or with the information, which may be accessed (for example, a classification level).


Access Modification
The security policies, and the rules established therein, that determine types of, and reasons for, modification to an entity's established right of access to a terminal, transaction, program, or process.

Accountability
The property that ensures that the actions of an entity can be traced uniquely to that entity.


TMA HIPAA Security Web Site

Final Rule (1 of 2)


[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)



Security Awareness Campaign


Check out the new [Password Management](#) poster for this month which can be found on the [Posters/Brochures](#) page.

Additional Resources


- [Security Awareness and Training](#)
- [Access Controls](#)
- [Person and Entity Information Access](#)
- [Security Definitions](#)
- [Final Rule](#)
- [Info Articles](#)
- [Policy/Guidance](#)

Important Message- HIPAA BASICS


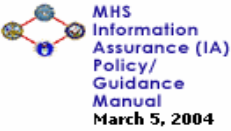
New upgrades are being made to the structure of the database, the process of reporting and new reports. Once implemented, enhanced reporting capabilities will be available that allow users to generate aggregate reports. A large portion of these upgrades involve the creation of new subscriptions and the movement of current gaps into a new hierarchy. The target dates for the migration to this new hierarchy is May 21, 2005 through May 24, 2005. **The HIPAA BASICS application will not be available during this time period.** In order to ensure that no gaps are lost during this transition we ask that no one create **new gaps, add new lead users, or reassign lead users after May 17, 2005**, until the upgrade is complete and the application is back on line. You may continue to work on gaps that already exist during the period between May 17, 2005 and May 21, 2005 when the application goes off line.

[The State of HIPAA Privacy and Security Compliance, April 2005 \(Survey\)](#) 

AHIMA has once again surveyed healthcare privacy officers and others whose jobs relate to HIPAA and relates to compliance with both the privacy and security rules. The results of the survey will reinforce the importance of protecting personal health information and help the industry to understand the areas of privacy and security implementation that are most difficult and may need more study.



- [SECURITY HOME PAGE](#)
- [PRIVACY HOME PAGE](#)
- [TMA GUIDANCE](#)
- [INFO LIBRARY](#)
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)



TMA HIPAA Security Web Site

Final Rule (2 of 2)



Federal Register

Thursday,
February 20, 2003

Part II

Department of Health and Human Services


Office of the Secretary

45 CFR Parts 160, 162, and 164
Health Insurance Reform: Security
Standards; Final Rule


TMA HIPAA Security Web Site

Info Articles (1 of 2)


[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)



Security Awareness Campaign


Check out the new [Password Management](#) poster for this month which can be found on the [Posters/Brochures](#) page.

Additional Resources


- [Security Awareness and Training](#)
- [Access Controls](#)
- [Person and Entity Information Access](#)
- [Security Definitions](#)
- [Final Rule](#)
- [Info Articles](#)
- [Policy/Guidance](#)

Important Message- HIPAA BASICS


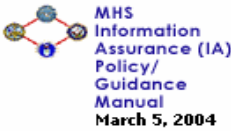
New upgrades are being made to the structure of the database, the process of reporting and new reports. Once implemented, enhanced reporting capabilities will be available that allow users to generate aggregate reports. A large portion of these upgrades involve the creation of new subscriptions and the movement of current gaps into a new hierarchy. The target dates for the migration to this new hierarchy is May 21, 2005 through May 24, 2005. **The HIPAA BASICS application will not be available during this time period.** In order to ensure that no gaps are lost during this transition we ask that no one create **new gaps, add new lead users, or reassign lead users after May 17, 2005**, until the upgrade is complete and the application is back on line. You may continue to work on gaps that already exist during the period between May 17, 2005 and May 21, 2005 when the application goes off line.

[The State of HIPAA Privacy and Security Compliance, April 2005 \(Survey\)](#) 

AHIMA has once again surveyed healthcare privacy officers and others whose jobs relate to HIPAA and relates to compliance with both the privacy and security rules. The results of the survey will reinforce the importance of protecting personal health information and help the industry to understand the areas of privacy and security implementation that are most difficult and may need more study.




- [SECURITY HOME](#)
- [PRIVACY HOME](#)
- [TMA GUIDANCE](#)
- [INFORMATION](#)
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)

 [Email Disclaimer Statement](#)

TMA HIPAA Security Web Site

Info Articles (2 of 2)

| | | |
|--|--|---|
|  HOME A to Z SEARCH HELP WHAT'S NEW SITE MAP | | |
|  TMA Privacy Office HIPAA Compliance: Security  | | |
| Home | INFORMATION ARTICLES |  SECURITY HOMEPAGE PRIVACY HOMEPAGE TMA GUIDANCE INFO LIBRARY NEWS & CONFERENCES TRAINING AND TOOLS SECURITY IPT POSTERS/BROCHURES FAQs LINKS CONTACT US   Email Disclaimer Statement |
| Freedom of Information Act (FOIA) | Data Security Guidelines Are Not Just For Healthcare | |
| Records Management | Secure Removal of PHI Cleaning Hard Drives to the HIPAA Standard Prior to Disposal or Donation | |
| HIPAA Compliance | HIPAA and Medical Record Copy Charges | |
| Privacy Act of 1974 | Final Security Regulations & How They Relate to the Privacy Rule | |
| System of Records | A Reasonable Approach to Security | |
| Data Use Agreements | HIPAA Compliance Doesn't Come in a Box | |
| Personnel Security (ADP Background Checks) | How HIPAA Security Policies Affect Corporate E-mail Systems | |
| | Best Practices in Healthcare Information Security for HIPAA Compliance | |
| | Password Management Best Practices | |
| | Choosing Good Passwords | |
| | Single Sign-on | |
| | Password Security Guidelines | |
| | Security Awareness and Training | |
| | Access Controls | |
| | Person and Entity Authentication | |
| | Information Access Management | |


TMA HIPAA Security Web Site

News and Conferences

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Compliance](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

NEWS & CONFERENCES

[News Archive](#) [Conference Disclaimer](#)

NEWS

[Hackers Shifting Their Focus to Pharming](#)
March, 23, 2005

[Secure Removal of Protected Health Information](#)

[Procedures for HIPAA Complaints: Offers Security Guidance](#)
This notice in the Federal Register, effective April 25, 2005, sets forth procedures for filing complaints of non-compliance with HIPAA Administrative Simplification provisions including:

- Transactions and Code Sets
- National Employer Identifier Number
- Security Rule
- National Plan Identifier Rule

This delegation **does NOT include complaints regarding non-compliance of the Privacy Rule.** Complaints dealing with privacy issues should be directed to TMA and or the Office of Civil Rights (OCR) and this information is available on the [HIPAA Forms](#) page.

CONFERENCES

Note: conferences noted with a () indicate the TMA Privacy Officer will be presenting information*

2005 HIPAA Training Conference
The dates for the first two HIPAA Training conferences will be July 11-14th in Bethesda, Maryland and July 25-28th in San Diego, California. Dates and locations for the September conferences have not yet been finalized; however there will be one week on the East coast and one week on the West coast. All registration will be pre-registration only and controlled through your service representative; there will be **NO on site registration.** New this year will be an advanced HIPAA track for the more experienced HIPAA practitioners you won't want to miss!

[HIPAA Security Too Little Too Late](#) 10th National HIPAA Summit Conference held from April 6-8, 2005



- [SECURITY HOMEPAGE](#)
- [PRIVACY HOMEPAGE](#)
- [TMA GUIDANCE](#)
- [INFO LIBRARY](#)
- [NEWS & CONFERENCES](#)**
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)



MHS Information Assurance (IA) Policy/Guidance Manual
March 5, 2004



Email Disclaimer Statement

TMA HIPAA Security Web Site

Training and Tools

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Compliance](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

TRAINING AND TOOLS

The TMA HIPAA program is evolving from implementation to compliance. Are you ready? To support you in your HIPAA compliance efforts, TMA offers training options such as live webcasts and online courses, as well as additional documentation to assist you in the learning process. Our course offerings will be expanded this year to include courses that will focus specifically on compliance efforts. Stay tuned!

Go to Tools
[LMS](#) / [HIPAA BASICS](#)

2005 HIPAA Training Conference

The dates for the first two HIPAA Training conferences will be July 11-14th in Bethesda, Maryland and July 25-28th in San Diego, California. Dates and locations for the September conferences have not yet been finalized; however there will be one week on the East coast and one week on the West coast. All registration will be pre-registration only and controlled through your service representative; there will be **NO on site registration**. New this year will be an advanced HIPAA track for the more experienced HIPAA practitioners you won't want to miss!

WebEx

To attend any live webcast, please contact your Service Representative to receive the invitation that includes all necessary login information.

- [WebEx directions](#)

Annual Training

- Security Training
- Annual Privacy Refresher Training

Training Materials Archive

- LMS Refresher Training
- 2004 Summer Training Presentations
- Quarterly Webex Training



- [SECURITY HOMEPAGE](#)
- [PRIVACY HOMEPAGE](#)
- [TMA GUIDANCE](#)
- [INFO LIBRARY](#)
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)



MHS
Information
Assurance (IA)
Policy/
Guidance
Manual
March 5, 2004




Email
Disclaimer
Statement


TMA HIPAA Security Web Site

Security IPT

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [WHAT'S NEW](#) [SITE MAP](#)



TMA Privacy Office HIPAA Compliance: Security



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

HIPAA Security Integrated Project Team (IPT)

A HIPAA Security Working Integrated Project Team (WIPT) was established in February 2001 to assist the Military Health System (MHS) with the implementation of HIPAA Security. It was re-chartered in the fall of 2003 to include the establishment of four specific subcommittees and was transitioned from a WIPT to an IPT in March 2004 after the disbandment of the HIPAA Overarching Integrated Project Team (OIPT). In the November 2003 issue of the [HIPAA Newsletter](#), each of the subcommittees were discussed in terms of their focus and responsibilities.

This page will provide you with an update of the IPT's most recent activities, announcements and upcoming events. The new Security IPT calendar will include meeting dates, conferences and deliverables.


HIPAA Security IPT Activities as of March 2005

Operations Sub-Committee


- The Compliance Assurance Framework is about to be entered into the signature process. It will need to be signed by Admiral Mayo.
- The Incident Response Plan is still being drafted. They hope to have that ready by the end of the month.
- The Governance Plan is still on hold.

Policy Sub-Committee


- The directive is still in the signature coordination process. It is currently located in the office of the TMA Chief of Staff.
- The regulation is also in the signature coordination process. It is currently located in the office of the TMA Chief of Staff.
- Comments were received from the Air Force, Army and TMA and changes based on those comments are currently being made. It will then be entered into the signature process.



- [SECURITY HOMEPAGE](#)
- [PRIVACY HOMEPAGE](#)
- [TMA GUIDANCE](#)
- [INFO LIBRARY](#)
- [NEWS & CONFERENCES](#)
- [TRAINING AND TOOLS](#)
- [SECURITY OFFICERS](#)
- [BA AGREEMENTS](#)
- [SECURITY IPT](#)
- [POSTERS/BROCHURES](#)
- [FAQs](#)
- [LINKS](#)
- [CONTACT US](#)



MHS Information Assurance (IA) Policy/Guidance Manual
March 5, 2004





Email Disclaimer Statement

TMA HIPAA Security Web Site

Posters/Brochures

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [SITE MAP](#) [SEE SOMETHING WRONG?](#)

 **TMA Privacy Office** 

[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[PIAs](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)


HIPAA Compliance and Marketing Materials


[NoPP Brochures - SmartSite](#)

Notice of Privacy Practices (NoPP) Posters
If you have not received your shipment of NoPP Posters, please contact PrivacyMail@tma.osd.mil with your POC and complete mailing address information (no PO boxes).


NoPP Labels
Labels are no longer available for order on the SmartSite. Below is a template for local reproduction of the label which is sized to scale and can be reproduced locally on **Avery Label #5163, 5263, 2163, 5923, 5963** (size: 2 inches x 4 inches).
[▶ Print Labels Here](#)

HIPAA Security Awareness Campaign
Theme of the Month: Integrity
Poster: "Password Management"
Additional Resources:
[Security Awareness and Training](#)
[Access Controls](#)
[Person and Entity Authentication](#)
[Information Access Management](#)


Previous Posters


Announcement
[POSTERS/BROCHURES](#)
[SUBSCRIBE TO E-NEWS](#)
[TRAINING & TOOLS](#)
[HIPAA QUICKGUIDES](#)
[SOR NOTICES](#)
[CONTACT US](#)

The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206
TRICARE benefit questions: questions@tma.osd.mil; Web site technical issues: webmaster@tma.osd.mil
The content of this page was updated on 20 May 2004.



TMA HIPAA Security Web Site

Poster Background

- Developed by HIPAA Security IPT Training and Education Subcommittee
- Purpose:
 - Aide in increasing awareness of good security practices
 - Target audience is information system users
 - Designed as a long term campaign (1 for each month of the year)
 - Designed to integrate into other existing training and awareness programs

TMA HIPAA Security Web Site

Poster Content

- Posters grouped into three themes: Confidentiality, Integrity, and Availability, with one comprehensive poster that combines all three
- Contemporary design to catch the eye
- One color for each theme
- Each poster has the theme, a topic, slogan and text

HIPAA Security Poster Campaign

Visitor Control Poster

**Question visitors
to protect patient
privacy and safety**



**INTEGRITY
VISITOR CONTROL**

Hospitals and clinics fill with people everyday. Take the time to ask lost or otherwise out-of-place individuals if they need assistance in finding their way. They won't mind if they have genuine reasons for visiting your facility. Patient privacy and safety will be ensured if you turn away persons who may have bad intentions.

Put HIPAA Security Official in:



www.tricare.osd.mil/tmaprivacy/hipaa/hipaasecurity

HIPAA Security Poster Campaign

Logoff Workstation Poster

**When leaving your workstation
unattended, logoff to preserve
confidentiality**

CONFIDENTIALITY
LOGOFF WORKSTATION

Many things can happen if you do not logoff your workstation when leaving. Unauthorized persons can view or modify patient information. An unsecured computer can compromise patient care, damage professional reputations, create extra work to repair the damage, and lead to lawsuits and fines. Take the time: logoff!

My HIPAA Security Official is:




HIPAA Security Awareness



www.tricare.osd.mil/tmaprivacy/hipaa/hipaasecurity

Information Security Requirements Poster

**Practice strong information security
to protect the integrity, availability
and confidentiality of patient health
information**






The image shows two men from behind, pushing a large, heavy computer system (monitor, tower, and printer) across a floor. The man on the left is wearing a light green shirt and dark pants, and the man on the right is wearing a red shirt and dark pants. They are both leaning forward, exerting effort to move the equipment. The computer system is a large, bulky unit with a CRT monitor on top and a printer attached to the side.

INFORMATION SECURITY REQUIREMENTS

HIPAA encourages us to remember that protecting the accuracy and completeness of patient information matters as much as protecting its confidentiality. Providing inaccurate or incomplete data to authorized persons could harm patients - so too could blocking access to accurate and complete data. Thus, a sound data security program protects the integrity and availability as well as the confidentiality of patient information.


My HIPAA Security Official is:

www.tricare.osd.mil/tmaprivity/hipaa/hipaasecurity

HIPAA Security Poster Campaign

Password Management Poster






Use appropriate passwords to guard against attacks

CONFIDENTIALITY
PASSWORD MANAGEMENT

DoD regulations require passwords of eight or more characters that have a mixture of upper and lower case letters, numbers, and special characters. To help you remember multiple passwords, develop an easily remembered system or pattern. Follow the rules and change your password regularly. Do not write passwords and leave them where they can be found and used by others.

My HIPAA Security Official is:

www.tricare.osd.mil/tmaprivacy/hipaa/hipaasecurity

TMA HIPAA Security Web Site

Poster Distribution

- Distributed once a month starting last year with a comprehensive poster
- Distribution coordinated with related information via e-newsletter
- 3 copies of each poster to each MTF
 - Limited number of additional posters available on request
- Mailed to each MTF's Privacy or Security Officer
- If not receiving posters contact privacymail@tma.osd.mil
- Electronic copies available on web site
- Currently on poster 10 of 12

How to Integrate Posters

- Review elements of your current programs and or resources to:
 - Determine which elements can be used to promote awareness of the posters (e.g., existing monthly staff newsletters)
 - Use posters and related material to support other programs that are related to either security or HIPAA
 - Build on poster themes and topics in your own awareness campaign
- Post in elevator lobbies and other high traffic areas
- Color printing is available from the TMA HIPAA Website in an 8.5x11 version

E-News (1 of 2)

- Electronic Mailing List to serve as additional resource for information and activities within TMA pertaining to maintaining the privacy and security of information held by its employees, military treatment facilities (MTFs) and business associates
- Subscribing members receive links to featured documents recently posted on the TMA Privacy Office web site
- Subscribing members also receive new privacy and security-related information in the general health care industry

TMA HIPAA Security Web Site

E-News (2 of 2)

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [SITE MAP](#) [SEE SOMETHING WRONG?](#)



TMA Privacy Office



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[PIAs](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

About E-NEWS

The TRICARE Management Activity (TMA) Privacy Office is now offering an electronic Mailing List to serve as an additional resource for information related to activities within TMA that protect the privacy and security of information held by its employees, military treatment facilities (MTFs) and business associates. Subscribing members will receive links to featured documents recently posted on the TMA Privacy Office website as well as new privacy and security-related information in the general health care industry. Please be assured that your contact information will be kept confidential as this is a private and secure TMA Mailing List. The TMA Privacy Office is committed to ensuring patient information privacy and security is sufficiently protected at every level as TRICARE delivers the best medical care possible to those we serve.

[Subscribe](#) / [Unsubscribe](#)

Or

[Back to Home](#)



Announcement

[POSTERS/BROCHURES](#)
[SUBSCRIBE TO E-NEWS](#)
[TRAINING & TOOLS](#)
[HIPAA QUICKGUIDES](#)
[SOR NOTICES](#)
[CONTACT US](#)

The TRICARE/Military Health System Web site www.tricare.osd.mil is the official Web presence of the Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE Management Activity Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3208

TRICARE benefit questions: questions@tma.osd.mil; Web site technical issues: webmaster@tma.osd.mil

The content of this page was updated on 22 January 2004.




HIPAA Quick Guides (1 of 2)

- Quick Guides are essentially credit card sized brochures which fold out (like a map) to display important HIPAA reference information
- These guides are intended for HIPAA Privacy and Security Officers as well as the general MHS workforce and they are not intended for beneficiary use


TMA HIPAA Security Web Site

HIPAA Quick Guides (2 of 2)

[HOME](#) [A to Z](#) [SEARCH](#) [HELP](#) [SITE MAP](#) [SEE SOMETHING WRONG?](#)



TMA Privacy Office



[Home](#)
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[PIAs](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

HIPAA Compliance and Marketing Materials

What is a HIPAA Quick Guide?
Quick Guides are essentially credit card sized brochures which fold out (like a map) to display important HIPAA reference information.


What information is contained on the HIPAA Quick Guides?
The TMA Privacy Office has developed two Quick Guides.

1. [Quick Guide to HIPAA Privacy and Security](#)
This card outlines the standards and implementation specifications found in the HIPAA Privacy Rule and DoD Health Information Privacy Regulation and lists the security standards and implementation specifications in the Security Rule.
2. [Quick Guide to Uses and Disclosures of PHI](#)
This card references the instances when the use of PHI can be used and disclosed without authorization from the individual.

Who can utilize these HIPAA Quick Guides?
These guides are intended for HIPAA Privacy and Security Officers as well as the general MHS workforce. They are not intended for beneficiary use.

How can we order these?
Because we have a limited quantity we are establishing a limit of 25 per organization. Please contact us at PrivacyMail@tma.osd.mil with a POC and street mailing list and we will be happy to send them to you.

We have begun the mailout of posters for the HIPAA Security Awareness Campaign! Every month, your HIPAA Security Official should receive three copies of that month's designated poster, each identifying a different theme pertaining to Availability, Confidentiality, or Integrity. If you have not yet received your posters, please contact PrivacyMail@tma.osd.mil to make sure we have your correct facility address and point of contact information.



POSTERS/BROCHURES

SUBSCRIBE TO E-NEWS

TRAINING & TOOLS

HIPAA QUICKGUIDES

SOR NOTICES

CONTACT US

TMA HIPAA Security Web Site

Summary

- You should now be able to:
 - Locate information pertaining to security topics and HIPAA security management
 - Locate information pertaining to HIPAA support tools and training
 - Locate information pertaining to HIPAA news, conferences and e-news

Risk Information Management Resource (RIMR)

Objectives

- Upon completion of this lesson, you should be able to:
 - Identify what systems and processes form RIMR
 - Describe the information the database stores and provides
 - Identify who developed the RIMR and how it helps you maintain compliancy

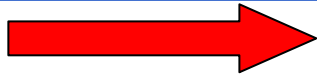
What is RIMR? (1 of 2)

- Web portal provides access to:
 - Information Assurance (IA) resources (policies, case studies, white papers)
 - Plans, Policies and Procedures Working Group (P3WG) HIPAA Privacy and Security Reports
 - Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVESM) (including methodology, automated tool, risk database and support center)
- OCTAVESM Automated Tool (OAT)
 - Downloads to desk top
 - Documents the results of each OCTAVESM and stores in database
 - Steps user through the process
 - Prints final reports

What is RIMR? (2 of 2)

- Risk Database
 - Stores completed risk assessments
 - Provides aggregate reports
 - Can be used to research common vulnerabilities
 - Trend analysis
 - Supports enterprise wide problem solving and mitigation
 - Justification for funding initiatives

Where is RIMR? - <http://rimr.tatrc.org>



- [Policy Library](#)
- [References](#)
- [Presentations](#)
- [Risk Assessment](#)
- [Training](#)
- [MISRT Training](#)
- [Technical Watch](#)
- [Coming Events](#)
- [C & A](#)
- [OCTAVEsm](#)
- [Information Center](#)
- [Site Search](#)
- [Home](#)

**RIMR**

RISK INFORMATION MANAGEMENT RESOURCES

Welcome to the Risk Information Management Resource (RIMR)!

RIMR enables the Department of Defense Military Health System to centrally manage and distribute worldwide access to a range of information sources for assessing, enhancing, studying and archiving data about defense health information assurance.

The primary audience for RIMR includes members of Medical Information Security Readiness Teams (MISRT) at all medical treatment facilities and defense, government and contractor employees with responsibility for protecting health information security.

RIMR includes the following resources:

Policy Library contains copies of all policies containing guidance on protecting the confidentiality, integrity, and availability of health care records and information from the Department of Defense, Army, Air Force, Navy. The policy library also has an authenticated webboard collaborative area.

Reference Library contains presentations, reports, documents and hyperlinks concerning important and interesting topics in health information assurance, such as the data security regulations of the Health Insurance Portability and Accountability Act of 1996. A search engine helps you efficiently use the Reference section.

Risk Assessments constitute the heart of information assurance. In this section, you will find the implementation guide for OCTAVEsm a self-directed information security risk assessment, the OCTAVEsm Information Center and capability to upload OCTAVEsm results to databases.

Training Center provides detailed information about future workshops on health information protection including logistical and registration details, HIPAA Training, and online Cyber Seminars.

Reference Library

[Policy Library](#)
[References](#)
[Presentations](#)
[Risk Assessment](#)
[Training](#)
[MISRT Training](#)
[Technical Watch](#)
[Coming Events](#)
[C & A](#)
[OCTAVEsm](#)
[Information Center](#)
[Site Search](#)
[Home](#)

REFERENCE LIBRARY

Welcome to the RIMR Reference Library!

The Reference Library contains multiple types of resources addressing issues in protecting the confidentiality, integrity and availability of health care records and information.

- [Presentations](#) includes power point slides of talks given by various individuals on the Department of Defense health information assurance program.
- [Reports](#) includes documents on specific topics in DoD health information assurance such as the Final Reports of the P3 Working Group that compare HIPAA data security and HIPAA privacy regulations with DoD and service policies.
- [Documents](#) includes resources from various sources on general and specific topics in health information assurance.
- [Hyperlinks](#) connects you directly to resources concerning health information assurance on the World Wide Web.

You may consult the Reference Library in two ways:

- Click on the type of resource you wish to consult and make a selection from the list of titles, or
- Use the [Search](#) engine that enables you automatically to find resources by author, title, subject or keyword.

RIMR OCTAVESM



| | |
|---|---|
| <ul style="list-style-type: none">Policy LibraryReferencesPresentationsRisk AssessmentTrainingMISRT TrainingTechnical WatchComing EventsC & AOCTAVESMInformation CenterSite SearchHome | <h2>RISK ASSESSMENT LIBRARY</h2> <p>Welcome to the RIMR Risk Assessments Library!</p> <p>The Risk Assessments Library contains a variety of resources designed to help you understand and execute information security risk assessments in your facility.</p> <ul style="list-style-type: none">• OCTAVESM Implementation Guide provides everything you need to execute a self-directed information security risk assessment at your facility, including detailed instructions, explanatory slides, worksheets, templates and examples.• Automated OCTAVESM Interface* enables you to enter and save results from OCTAVESM workshops directly into a computerized database.• OCTAVESM Information Center provides online information and support as you use OCTAVESM to improve health information assurance in your facility.• Other risk assessment tools* provides information about other tools available for information security risk assessment. |
|---|---|

Who Developed RIMR

- Congressionally funded through Defense Health Information Assurance Program (DHIAP)
- Currently located at Ft. Detrick
- DoD owned – not vender owned
- Developers
 - Advanced Technology Institute, Charleston SC
 - KRM Associates, Inc, Shepherdstown WV
 - Software Engineering Institute at Carnegie Mellon (CERT), Pittsburgh PA

P3WG Final Report Background

- DHIAP and the DoD/HA HIPAA Overarching Integrated Process Team (OIPT) sponsored the formation of the interdisciplinary and inter-service Policies, Procedures, and Practices Workgroup
- Compared all pertinent DoD and service level regulations with the HIPAA Data Security Rule
- Identified gaps and discrepancies and made recommendations for changes

P3WG Final Report Content

- Executive summary and methodology
- Chapter for each rule and associated implementation specifications
 - HIPAA wording with plain English explanation
 - All mapped citations
 - Compliance analysis with recommendations
- Analysis of results

P3WG Final Report Utilization

- Used at multiple levels
- Guide central policymakers in making revisions
- Critical input includes analysis of results and recommendations
- Use as background information when updating local policies
 - Identifies upper level policies and procedures MTF's should follow
 - Identifies gaps local policies and procedures must fill
- Feed remaining gaps into risk analysis

Summary

- You should now be able to:
 - Identify what systems and processes form RIMR
 - Describe the information the database stores and provides
 - Identify who developed the RIMR and how it helps you maintain compliancy

HIPAA Security Implementation Guide

HIPAA Security Implementation Guide

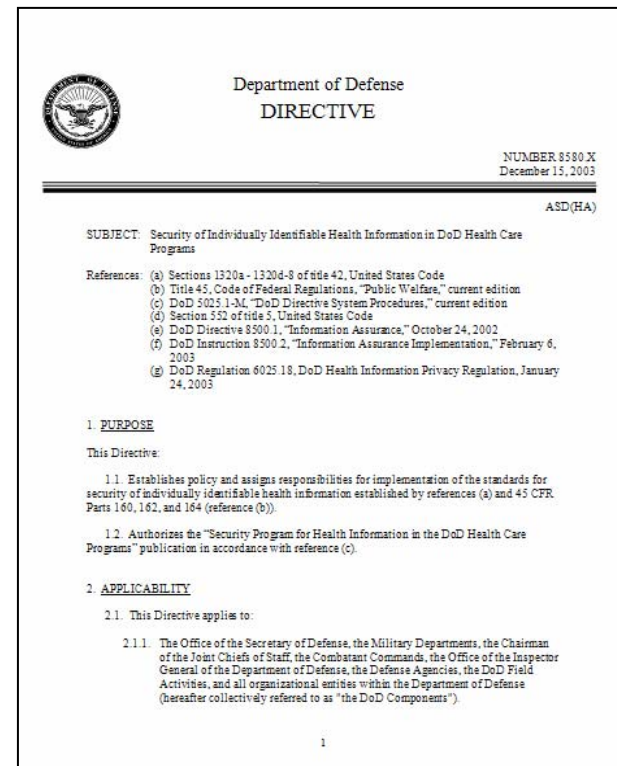
Objectives

- Upon completion of this lesson, you should be able to:
 - Identify the purpose and organization of the Implementation Guide

HIPAA Security Implementation Guide

Purpose (1 of 3)

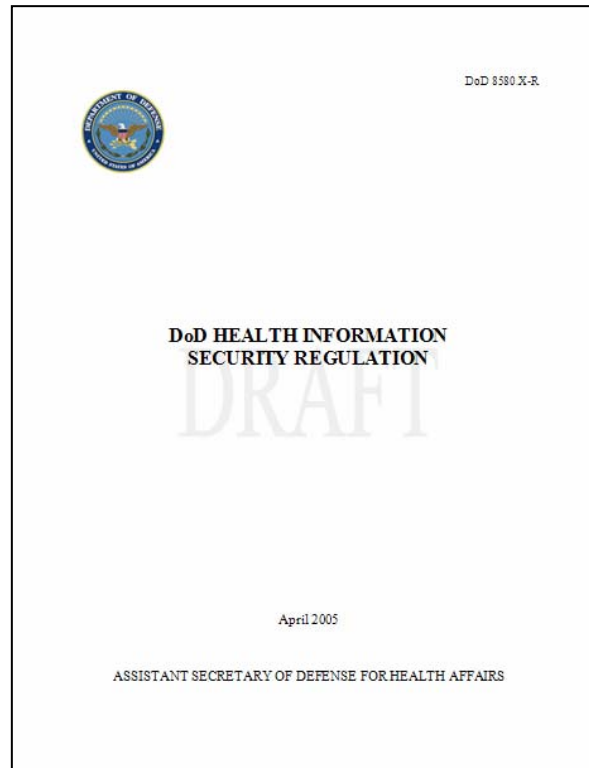
- Provide guidance with the implementation of:
 - DoD 8580.X-D, Security of Individually Identifiable Health Information in DoD Health Care Programs



HIPAA Security Implementation Guide

Purpose (2 of 3)

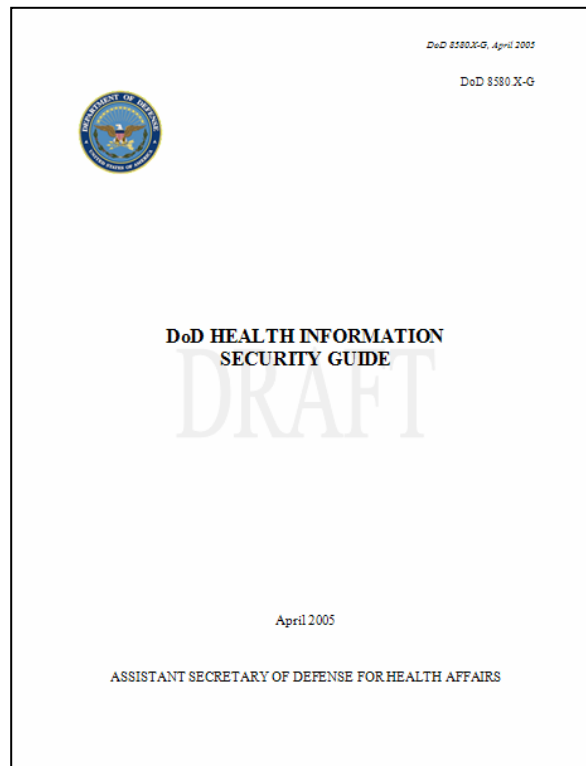
- Provide guidance with the implementation of (Cont.)
 - DoD 8580.X-R, DoD Health Information Security Regulation



HIPAA Security Implementation Guide

Purpose (3 of 3)

- Contains “actionable steps” towards compliance



HIPAA Security Implementation Guide

Organization of Guide (1 of 3)

- Chapter 1: General Information
 - Background
 - History of HIPAA
 - What is HIPAA Security
 - Definition
 - Key concepts and terms
 - Organization of requirements within the security rule
 - Compliance
 - How to achieve HIPAA Security compliance

HIPAA Security Implementation Guide

Organization of Guide (2 of 3)

- Chapter 1: General Information (cont.)
 - Existing DoD Requirements
 - Explanation of why most HIPAA security standards and implementation specifications are required and not addressable
- Chapter 2: Administrative Safeguards
 - Administrative standards and implementation specifications with general guidance on how to achieve compliance
- Chapter 3: Physical Safeguards
 - Physical standards and implementation specifications with general guidance on how to achieve compliance

Organization of Guide (3 of 3)

- Chapter 4: Technical Safeguards
 - Technical standards and implementation specifications with general guidance on how to achieve compliance
- Chapter 5: Policies and Procedures, and Documentation
 - Policies and Procedures, and Documentation standards and implementation specifications with general guidance on how to achieve compliance

Organization of Standards (1 of 4)

- C2.2. ASSIGNED SECURITY RESPONSIBILITY

The number and type of personnel required to implement an organization's security policies in a manner consistent with reference (e) depends on the size and structure of the organization. Document and validate the actual workforce numbers with a breakdown of responsibilities as part of the security management process. The HIPAA Security regulation states the following:

Organization of Standards (2 of 4)

- C2.2.1. Policy - Identify and assign in writing the security official for the organization who is responsible for the development and implementation of the policies and procedures required by this Regulation. While more than one individual may be given security responsibilities, a single individual must be designated as having the overall final responsibility.

- C2.2.2. Guidance
 - C2.2.2.1. Step 1: Security Official - Select a security official. The ideal candidate should demonstrate competency in the following areas:

Organization of Standards (3 of 4)

- C2.2.2.1.1. Ability to communicate effectively with and coordinate the efforts of technology and non-technology personnel
 - C2.2.2.1.2. General understanding of hardware and software security, as well as physical security.
 - C2.2.2.1.3. Familiarity with the legal requirements relating to security and health care operations
- C2.2.2.1. Step 2 - Roles and responsibilities. Assign roles and responsibilities. **Table C2.T6.** below is a general description of Security Officer roles and responsibilities.

Organization of Standards (4 of 4)

| HIPAA Security Officer Roles and Responsibilities | |
|--|--|
| Oversee Policy Implementation, Oversight, Reviewing and Compliance | |
| | Manage the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule. |
| | Identify and review the security features of existing and new computing systems to ensure that they meet the security requirements of existing policies. Review and propose changes to existing policies and procedures that reflect the existing requirements of the systems to which they apply. Periodically reassesses status and updated security standards established by the facility |
| | Monitor day-to-day entity operations and systems for compliance. Report to management on the status of compliance |
| | Periodically assess current security compliance status vs. necessary status (gap analysis). |
| | Work with management, the medical staff, the director of health information management, the privacy officer (if appointed separately), and others to ensure protection of patient privacy and confidentiality in a manner that does not compromise the entity, its personnel, good medical practice, or proper health information management practices. |

HIPAA Security Implementation Guide

Appendix 1 (1 of 3)

- Appendix 1: Crosswalk of HIPAA to DoD Regulations

| Standard | | Implementation Specifications | Regulatory Guidance | | | |
|----------|--|---------------------------------|---|--|--|--|
| Ref # | HIPAA Safeguards and Requirements | | Related DoD/MHS Policy | Related Air Force Policy | Related Army Policy | Related Navy Policy |
| | Administrative | | | | | |
| 1 | Security Management Process § 164.308(a)(1) | 1.0 Security Management Process | DoD 5160.54-D DoD 5200.40-I DoD 8500.1-D DoD 8500.2-I DoD 8000.1-D MHS IA Policy/Guidance Manual | AFD 33-2 AFI 33-201 AFI 33-202 AFI 33-207 AFI 41-210 | AR 25-2 AR 25-2 Best Business Practices | SECNAVINST 5239.3 OPNAVINST 5239.1B OPNAVINST 5530.14C BUMEDINST 5239.1 NAVMED P-117 Ch 16 |
| | | 1.1 Risk Analysis | DoD 5160.54-D DoD 5200.40-I DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual | AFD 33-2 AFI 33-201 AFI 33-202 AFSSI 5024 v.1 | AR 25-2 AR 25-2 Best Business Practices | SECNAVINST 5510.36 OPNAVINST 5239.1B OPNAVINST 5530.14C BUMEDINST 5239.1 |
| | | 1.2 Risk Management | DoD 5000.1-D DoD 5000.2-R DoD 5160.54-D DoD 5200.40-I DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual | AFI 33-202 AFSSI 5024 v.1 | AR 25-2 AR 25-2 Best Business Practices AR 40-66 | SECNAVINST 5510.36 OPNAVINST 5239.1B OPNAVINST 5530.14C BUMEDINST 5239.1 |

HIPAA Security Implementation Guide

Appendix 1 (2 of 3)

| Standard | | Implementation Specifications | Regulatory Guidance | | | |
|----------|--|--|---|---|---|--|
| Ref # | HIPAA Safeguards and Requirements | | Related DoD/MHS Policy | Related Air Force Policy | Related Army Policy | Related Navy Policy |
| | | 1.3 Sanction Policy | DoD 5000.2-R DoD 8510.1-M | AFI 33-129 AFJI 31-102 | AR 25-2 AR 25-2 Best Business Practices AR 40-66 AR 190-16 | BUMEDINST 5239.1 NAVMED P-117 Ch 16 |
| | | 1.4 Information System Activity Review | DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual | AFI 33-202 AFM 33-229 AFSSI 5027 | AR 25-2 AR 25-2 Best Business Practices AR 40-66 | No policy available. See related DoD policy. |
| 2 | Assigned Security Responsibility § 164.308(a)(2) | 2.0 Assigned Security Responsibility | DoD 5200.40-IDoD 8000.1-DDoD 8500.1-DDoD 8500.2-IDoD 8510.1-MMHS IA Policy/Guidance Manual | AFD 33-2AFI 33-119AFI 33-202AFI 41-210AFJI 31-102AFSSI 5024 v.1AFSSI 5027AFM 33-223 | AR 25-2 AR 25-2 Best Business Practices AR 190-16 | SECNAVINST 5239.3SECNAVINST 5510.36OPNAVINST 5239.1BOPNAVINST 5530.14CBUMEDINST 5239.1NAVMED P-117 Ch 16 |
| 3 | Workforce Security § 164.308(a)(3) | 3.0 Workforce Security | DoD 5200.2-D DoD 5200.2-R DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual | AFI 33-202 AFSSI 5027 | AR 25-2 AR 25-2 Best Business Practices AR 40-66 | SECNAVINST 5510.30 BUMEDINST 5239.1 |
| | | 3.1 Authorization and/or Supervision | DoD 8500.2-I DoD 8510.1-M | No Air Force policy available. See related DoD policy. | AR 25-2 AR 25-2 Best Business Practices | No policy available. See related DoD policy. |

HIPAA Security Implementation Guide

Appendix 1 (3 of 3)

| Standard | | Implementation Specifications | Regulatory Guidance | | | |
|----------|---|---|---|---|---|--|
| Ref # | HIPAA Safeguards and Requirements | | Related DoD/MHS Policy | Related Air Force Policy | Related Army Policy | Related Navy Policy |
| | | 3.2 Workforce Clearance Procedure | DoD 5200.2-D DoD 5200.2-R DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual | AFI 33-119 AFI 33-202 AFSSI 5027 | AR 25-2 AR 25-2 Best Business Practices | SECNAVINST 5510.30 BUMEDINST 5239.1 |
| | | 3.3 Termination Procedures | DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual | AFM 33-223 | AR 25-2 AR 25-2 Best Business Practices | SECNAVINST 5510.30 |
| 4 | Information Access Management § 164.308(a)(4) | 4.0 Information Access Management | DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual | AFI 33-202 AFSSI 5027 | AR 25-2 AR 25-2 Best Business Practices | SECNAVINST 5510.36 OPNAVINST 5239.1B NAVMED P-117 Ch 16 |
| | | 4.1 Isolating Clearinghouse Function | N/A | N/A | N/A | N/A |
| | | 4.2 Access Authorization | DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual | AFI 33-202 AFI 41-210 AFM 33-223 AFSSI 5027 | AR 25-2 AR 25-2 Best Business Practices | SECNAVINST 5510.36 BUMEDINST 5239.1 NAVMED P-117 Ch 16 |
| | | 4.3 Access Establishment and Modification | DoD 8500.2-I MHS IA Policy/Guidance Manual | AFI 33-202 AFI 41-210 | AR 25-2 AR 25-2 Best Business Practices | BUMEDINST 5239.1 |
| 5 | Security Awareness and Training § 164.308(a)(5) | 5.0 Security Awareness and Training | DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual | AFD 33-2 AFI 33-202 AFI 33-204 AFJI 31-102 AFM 33-223 | AR 25-2 AR 25-2 Best Business Practices AR 190-16 | SECNAVINST 5239.3 SECNAVINST 5510.30 SECNAVINST 5510.36 OPNAVINST 5239.1B OPNAVINST 5530.14C BUMEDINST 5239.1 NAVMED P-117 Ch 16 |

HIPAA Security Implementation Guide

Summary

- You should now be able to:
 - Identify the purpose and organization of the Implementation Guide

HIPAA Security and Biomedical Devices

HIPAA Security and Biomedical Devices

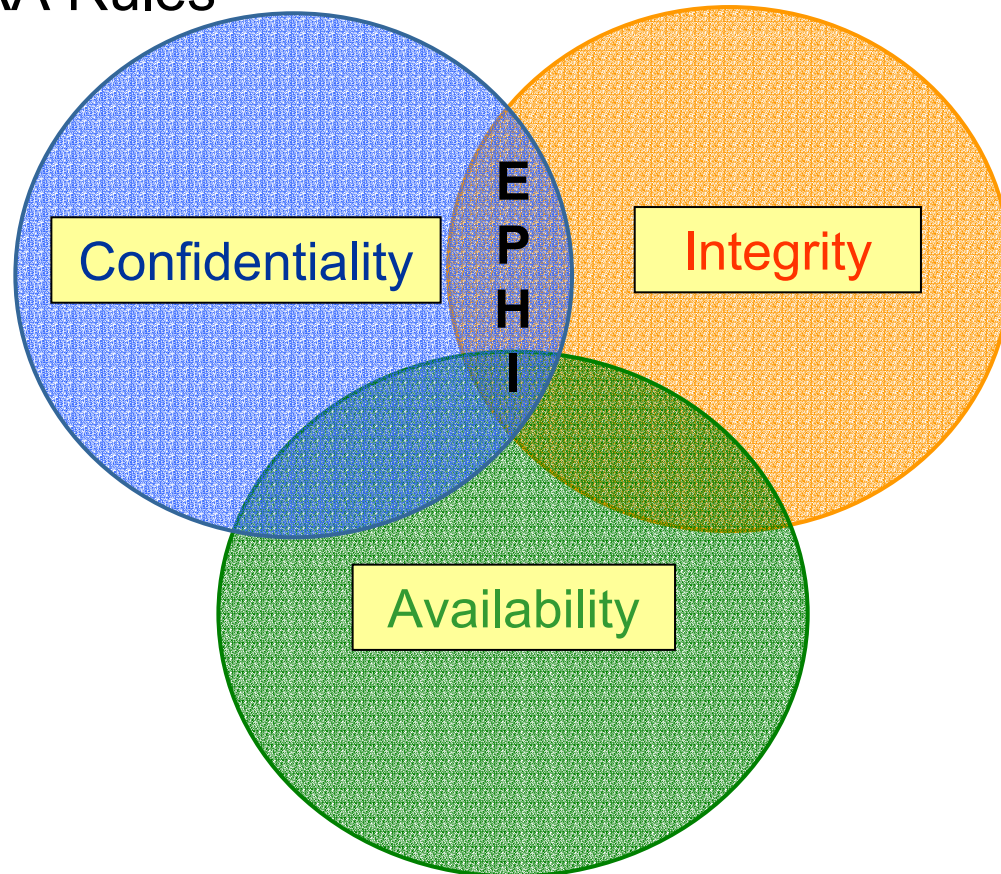
Objectives



- Upon completion of this lesson, you should be able to:
 - Describe the relationship between HIPAA security and biomedical devices
 - Detail the risks of using biomedical devices
 - Identify approaches for minimizing these vulnerabilities

HIPAA Security Requirement

- Must protect the confidentiality, integrity, and availability of any electronic health information that is protected under the HIPAA Rules



HIPAA Security and Biomedical Devices

Where is EPHI Found?

- Workstations
- Laptops
- Modems
- Databases
- Digitally recorded voice messages
- Computer-based facsimiles
- Servers
- Applications
- Network connections
- PDAs
- ***Biomedical devices***
- Compact disks
- Floppy diskettes

.....and many more!

HIPAA Security and Biomedical Devices

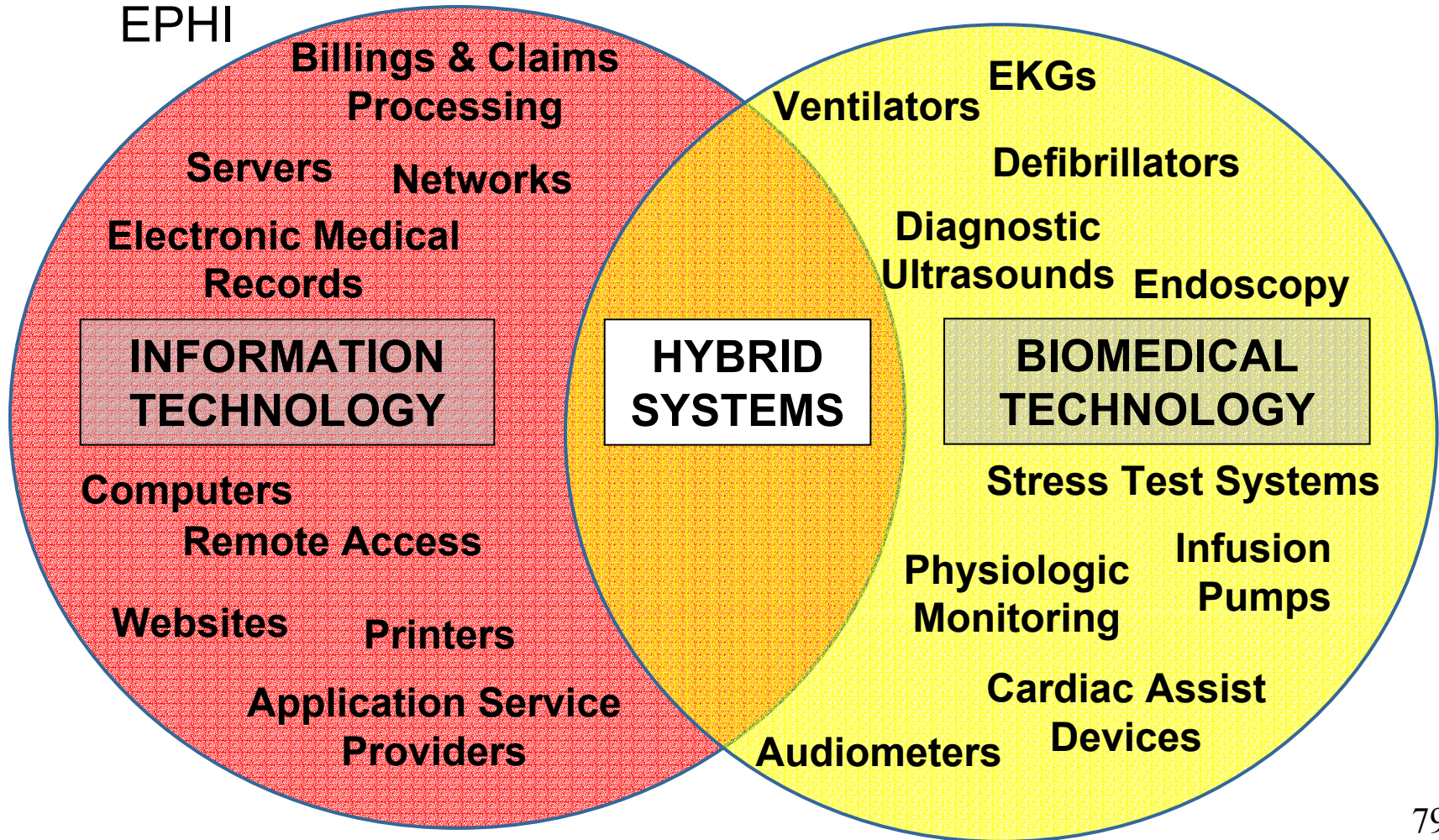
Biomedical Devices

- A biomedical device is defined as “...an instrument which is intended for use in the diagnosis of disease, or other conditions, or in the cure, mitigation, treatment or prevention of disease...” (Food and Drug Administration, 1989)
- Majority of these instruments are highly automated and collect and store health information



HIPAA Security and Biomedical Devices Systems

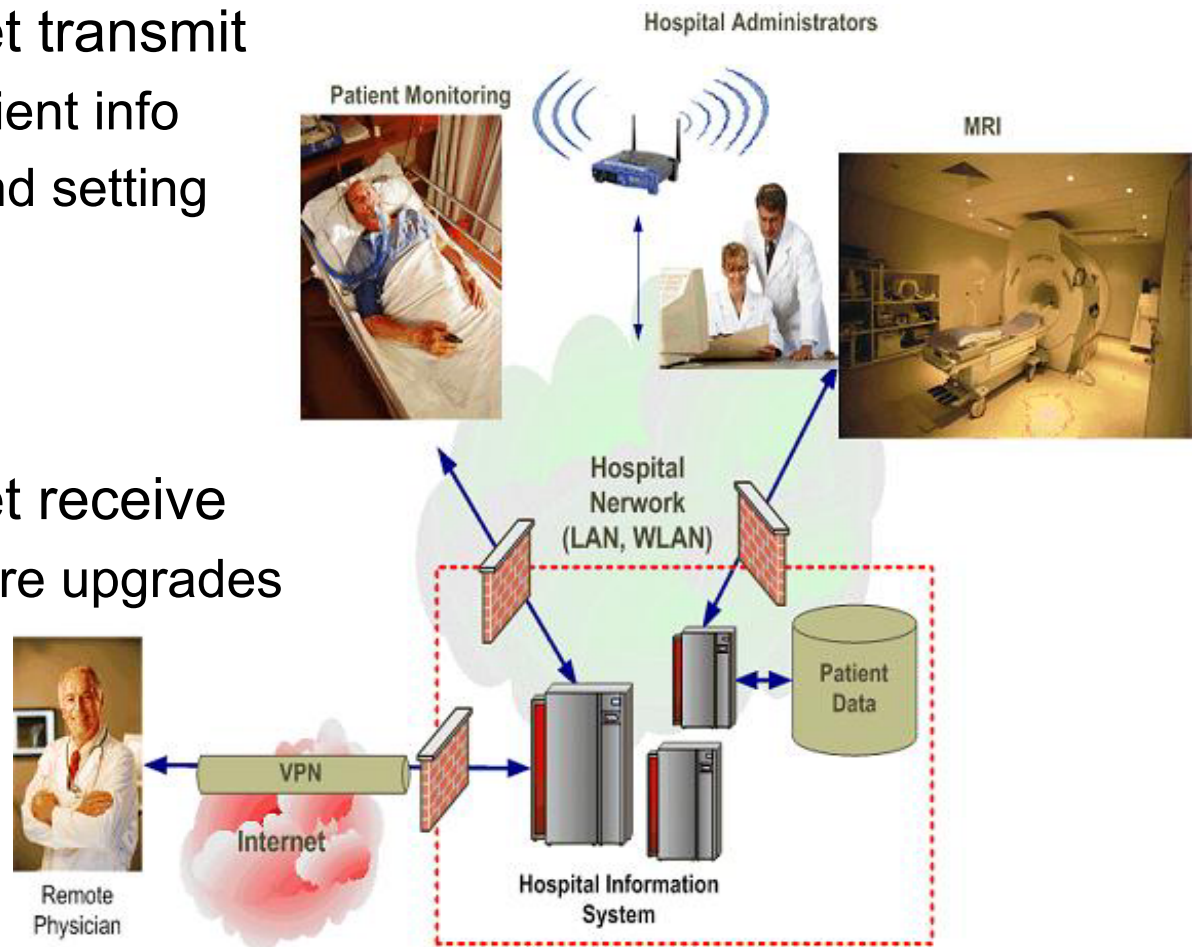
- Examples of devices/systems maintaining and transmitting EPHI



HIPAA Security and Biomedical Devices

Biomedical Devices and IT Systems

- Devices on Internet transmit
 - Location and patient info
 - Current status and setting
 - Diagnostics
 - Error codes
- Devices on Internet receive
 - Software/Firmware upgrades
 - Calibration
 - Diagnostics



HIPAA Security and Biomedical Devices

Historical Perspective

- Biomedical devices utilized at MTFs operated either as stand-alone devices or as networked devices on isolated medical networks
- As such, biomedical devices with unresolved software vulnerabilities posed little or no security threat



HIPAA Security and Biomedical Devices

Current Perspective

- Potential threats
 - Migration of biomedical devices into interconnected networks
 - Subject to vulnerability alerts and patching requirements
 - Unresolved software vulnerabilities due to FDA regulations



HIPAA Security and Biomedical Devices

Security Risks (1 of 2)

- Biomedical devices
 - Frequently store EPHI, and therefore, must be considered when implementing a comprehensive IT security program
 - Designated and operated as special purpose computers
 - More features are being automated and increasing amounts of PHI is being collected, analyzed, and stored
 - Growing integration and interconnection of different biomedical devices and IT systems where EPHI is being exchanged

HIPAA Security and Biomedical Devices

Security Risks (2 of 2)

- “In its report covering security threats during the first quarter, McAfee's Anti-virus and Vulnerability Emergency Response Team (AVERT) said Monday that more than 1,000 new attacks aimed at software vulnerabilities emerged in the first three months of this year ” (CNET)
 - Blended threats continue to constitute the most frequently reported threat
 - Combine the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack



HIPAA Security and Biomedical Devices Issues

- FDA requires vendors of medical devices to evaluate the impact of software changes on a medical device's safety and effectiveness before installing a security patch or upgrade
 - Vendors do not include this type of repair and testing in standard maintenance agreement
 - Evaluation entails unanticipated costs and effort
 - Most computerized medical devices are non-compliant with these FDA requirements

HIPAA Security and Biomedical Devices

Impact: Organization

- **Risk assessment**
 - MTFs must evaluate the threat to and from biomedical devices in the context of their wider approach to risk management
- **Equipment lifecycle management**
 - Security requirements must be included in contracts or Memorandums of Understanding/Agreement
 - Evaluation and remediation of vulnerabilities must be conducted before the installation of devices on the network
- **Contracts**
 - Must accommodate need for security upgrades to relevant equipment as appropriate and affordable

HIPAA Security and Biomedical Devices

Impact: Architecture

- Multiple, overlapping controls must be developed to support Defense-in-Depth
- Biomedical devices that acquire, distribute, display and archive medical information should be placed on their own physical or virtual segment of the network
- Precise configuration of the medical enclave depends on architectural rules of the wider network

HIPAA Security and Biomedical Devices

Recommendations (1 of 2)

- Share information on solutions amongst your peers
 - FDA Guidance related to approved vendors
 - The impact is obvious – the more you share amongst your peers, the more time and resources you save
 - Information sharing should not be limited to individual Services but across the MHS



HIPAA Security and Biomedical Devices

Recommendations (2 of 2)

- Develop new requirements in vendor maintenance contracts to cover vulnerability alerts
 - Future contracts should require patches as a component of maintenance
 - Sit down with your vendor and agree on an approach to patching biomedical devices.
- **NOTE:** Precedence for vendors to accept this responsibility has not been established – this is especially true with legacy systems

HIPAA Security and Biomedical Devices

Community Efforts to Address Issues

- Healthcare Information and Management Systems Society (HIMSS)
 - Biomedical Device Security Taskforce
 - <http://www.himss.org/content/files/deviceSecurity/MDSBiography.pdf>
- National Electrical Manufacturers Association (NEMA)
 - Joint Committee on Privacy and Security
 - <http://www.nema.org/prod/med/security/>
- NIST/WEDI/URAC
 - Biomedical Device Security Workgroup
 - http://www.urac.org/committees_sworkgroup.asp?navid=committees&pagename=committees_workgroups

HIPAA Security and Biomedical Devices

Summary

- You should now be able to:
 - Describe the relationship between HIPAA security and biomedical devices
 - Detail the risks of using biomedical devices
 - Identify approaches for minimizing these vulnerabilities



Training Summary

- You should now be able to:
 - Identify available resources to aid in Security Awareness
 - Identify available training briefings
 - Identify available resources to aid in implementation of HIPAA Security
 - Describe the relationship between HIPAA Security and biomedical devices

Resources

- Title 45, Code of Federal Regulations, “Health Insurance Reform: Security Standards; Final Rule,” Parts 160, 162 and 164, current edition
- www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- <http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm> to subscribe to the TMA Privacy Office E-News
- Service HIPAA Security Representatives

Additional Resources

- RIMR
 - <https://rimr.tatrc.org>
- HIMSS
 - <http://www.himss.org/content/files/deviceSecurity/MDSBibliography.pdf>
- NEMA
 - <http://www.nema.org/prod/med/security>
- URAC
 - http://www.urac.org/committees_sworkgroup.asp?navid=committees&pagename=committees_workgroups



HEALTH AFFAIRS



Please fill out your critique

Thanks!

